**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 294**

**SECURITY SOFTWARE**

**Describe each of the following software-based security types.**

1. **Encryption software**

Messages can be encrypted by using an algorithm so that the message is a meaningless jumble of characters to anyone who receives it.

* 1. **What are the two types of modern encryption methods?**
  + ***Symmetric-key encryption*** is where the sender & receiver have the same key installed on their computers
  + ***Asymmetric-key encryption***, (aka. public-key encryption) is where the sender encrypts a message or file using recipient’s public key and then the recipient decrypts the message using their private key.

1. **Network policies, profiles**

Users on a network will have a username and password that they use to access the information. The organisation can then control what each user can access.

1. **Firewalls**

A firewall is based on a combination of hardware and software that will only allow authorised network traffic to pass through the firewall. Firewalls may also provide protection against viruses and hackers.

1. **Antivirus software**

Antivirus softwarecan be used to prevent computer virus infections. The software detects the presence of a virus as the computer boots up, when an executable file is run, when documents are accessed or when files are copied

**SECURITY PROCEDURES, P 299**

**Communication**

1. **List the security considerations for communication within an organisation.**

The recent advances in technology allows communication without any real restriction.

**Storage**

1. **Filenaming conventions**
   1. **List the 3 types of information each document should include.**

* Date stamp
* Variation
* Name
  1. **Give an example of a sequential file-naming convention.**

Newsletter\_2011\_03oct.doc

1. **Location of files**

There must be a structure to the document location, the folders must be names appropriately and be easy to find.

1. **Backups**
   1. **Distinguish between each of the following:**
      1. **Full backup**

Full backup back up all files

* + 1. **Differential backup**

Differential backup backs up the files that have changed since last full backup and it only uses only 2 media. The restoration of files involves restoring files from the full backup and then from the differential backup.

* + 1. **Incremental backup**

Incremental backup backs up the files that have changed since the last incremental backup.

1. **Backup timeline**
   1. **List good practice in relation to backup timelines.**

* Perform as soon as the file has been changed
* Clearly label all back up media so that you know when the backup was made and what is on it.

1. **Location of backup files**
   1. **List good practice in the relation to the storage of backup files.**

* It is important to ensure that your backups work and run efficiently
  1. **What is the grandparent-parent-child system?**

This systems keeps different versions of each file, the child being the most recent. An incremental backup is preformed after each day and a differential back up after each week. A full back up is done at the end of each month.

1. **Archiving and destruction**
   1. **Distinguish between archiving and destruction?**

Archiving is essentially a process of copying files to long term storage then deleting them from the hard disk. Destruction involves the deleting only.

* 1. **What is a problem for ICT managers?**

ITC managers must ensure that they choose the most appropriate storage media.

* 1. **What is a legacy system?**

A legacy system refers to an old system that is still running.

1. **Disposal**
   1. **What issues must organisations consider in disposing information?**

Organisations must ensure that their data is properly disposed of and deleted fully. Sometimes information is not fully disposed and com be recovered from a hard dirve. Information needs to be properly disposed of so that the information is not read by a unintended person.